Department of Homeland Security Daily Open Source Infrastructure Report for 20 July 2005

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports an American Airlines flight to San Juan returned to Fort Lauderdale on Monday, after about an hour into the flight, when a threatening note was found on board. (See item 10)
- The Associated Press reports an investigation has resulted in the arrests of 40 Northern California pilots who may have been flying with debilitating illnesses that should have kept them grounded. (See item 11)
- ComputerWeekly reports the London bombing highlighted important gaps in business continuity plans, such as mobile phone networks that were out of action or unreliable for most of the day the bombs exploded. (See item 27)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 19, WOI−TV (IA)* — **Bomb scare at substation.** A bomb scare in a neighborhood in Des Moines, IA, on Monday, July 18, turned out to be a false alarm. Around 4 p.m. police were called to check out a bombshell found at E. 23rd and Logan. Police say it was inside a Mid American Energy substation. The bomb squad was brought in, but an x−ray showed it was a

dud. Police don't know from where the bombshell came.
Source: http://www.woi−tv.com/Global/story.asp?S=3608973&nav=1LFXcGu 7

2. *July 19, Associated Press* — **Vermont utilities urge power use reductions.** Several Vermont utilities are calling on customers to cut power usage on Tuesday, July 19, as demand for electricity in New England is expected to set a new record. The region is expected to have a peak load of 25,725 megawatts. That would beat the region's previous record power demand by 400 megawatts. Burlington Electric Department, Central Vermont Public Service and Green Mountain Power issued a statement asking customers to take steps to reduce power demand.
Source: http://www.wcax.com/Global/story.asp?S=3612432

3. *July 18, Associated Press* — **Dedicated trains to be used for nuclear waste shipments according to government agency.** Nuclear waste will be shipped to a national repository in the Nevada desert on dedicated railroad cars, rather than sharing trains with other cargo, the Department of Energy (DOE) announced Monday, July 18. Although general freight trains will be an option, DOE's policy will be to use dedicated trains for the estimated 3,500 shipments of spent nuclear fuel and high−level defense waste bound for the Yucca Mountain repository, the department said. The trains will carry waste from sites in some three−dozen states to the repository planned 90 miles northwest of Las Vegas. In addition to the train shipments, some 1,100 truck shipments will be needed, though they won't be affected by the transportation policy, officials said. Using dedicated trains will be cheaper and more secure than regular freight trains, department officials said. Yucca Mountain is planned as a national repository for 77,000 tons of nuclear waste to be buried for 10,000 years and beyond.
Source: http://www.lasvegassun.com/sunbin/stories/nevada/2005/jul/18 /071810895.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *July 18, WTHITV (IN)* — **Terre Haute firefighters tour local chemical company.** Firefighters want to make sure they know the ins and outs of Ulrich Chemical Inc., in Terre Haute, IN, in case of a fire. The company invited the firefighters to take part in a class where they were introduced to the chemicals housed at the plant. The department says it's important training, because on certain chemicals, water acts as a fuel to a fire. "The main objective here is to find out what all they have in here in the building, and what we can use water on and what we can't, because you can have a fire and not be able to use water," says Jeff Fisher of the Terre Haute Police Department.
Source: http://www.wthitv.com/newsdet.asp?id=9232

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *July 18, IDG News Service* — **Internet users ignorant about data privacy.** Internet users in the United States are dangerously ignorant about the type of data that Website owners collect from them and how that data is used, making them vulnerable to fraud and misuse of their personal information, a new study finds. For the study, titled "Open to Exploitation: American Shoppers Online and Offline," 1,500 adult U.S. Internet users were asked true−or−false questions about topics such as Website privacy policies. The survey was conducted by the University of Pennsylvania's Annenberg Public Policy Center. Respondents generally failed the test, answering an average of seven out of 17 questions correctly. The study's interviews, conducted between early February and mid−March, yielded findings the authors consider alarming, including 75 percent wrongly believe that if a Website has a privacy policy, users' information will not be shared with third parties, and 49 percent can't identify phishing scam e−mail messages. To address the problems identified in the study, the authors propose increased consumer education, as well as new regulations requiring retailers to disclose what data they have collected about customers and when and how they will use it.
   Study: http://www.annenbergpublicpolicycenter.org/04_info_society/Turow_APPC_Report_WEB_FINAL.pdf
   Source: http://www.infoworld.com/article/05/07/18/HNdataprivacy_1.html?source=rss&url=http://www.infoworld.com/article/05/07/18/ HNdataprivacy_1.html

6. *July 18, USA Today* — **Hackers shift focus to swiping ID information.** Computer attacks cost U.S. companies, government agencies and universities far less than they did a year ago, a new survey says. However, what was good for them may be bad for consumers and employees. Figures from the Computer Security Institute (CSI), an organization of information−security professionals, and the FBI show that more computer systems are better prepared to identify and fend off computer attacks. Yet the report also concludes that profit−minded hackers are targeting enterprises with large customer and employee databases. "The crooks are shifting their focus" to stealing the personal information of individuals, says Robert Richardson, CSI's editorial director. Hackers are stealing proprietary data with greater frequency by exploiting holes in Websites and applications, and through phishing, says Erik Caso, vice president of business development at NT Objectives, a computer−security company. The survey supplies more evidence that fraud is proliferating on the Internet, as thieves find new ways to exploit security weaknesses associated with online transactions. Police say one type of criminal specializes in stealing names, addresses, birth dates, driver's license numbers, Social Security numbers, account logons and passwords. Another type makes use of stolen IDs to finance all aspects of elaborate schemes to move electronic goods and cash out of the USA.
   To order a free copy of the survey: http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml
   Source: http://www.usatoday.com/money/industries/technology/2005−07−18−security−usat_x.htm

7. *July 18, CNN/Money* — **Americans guard against identity theft according to poll.** A majority of Americans fear the threat of identity theft and are doing something about it, according to a recent poll conducted by Money magazine and ICR. The telephone poll, which surveyed a little more than 1,000 individuals in June, revealed that 78 percent of those interviewed expressed concern that their identity may be stolen. Only eight percent of those interviewed claimed to have been a victim of identity theft. Ninety−six percent of Americans

said they have taken some precautionary measure to protect their personal information. Topping the list of precautions was shredding personal documents −− 80 percent of those surveyed said they destroyed papers with personal information. The other most popular deterrents were refusing to share Social Security numbers, not giving out personal information online and requesting companies not share data with outside firms.
Poll results: http://www.icrsurvey.com/ICRInTheNews/Money_ICR_poll_0705.ht ml
Source: http://money.cnn.com/2005/07/18/pf/security_identity_poll/in dex.htm?section=money_latest

[Return to top]

Transportation and Border Security Sector

8. *July 19, Washington Post* — **Dogs remain the best detectors of bombs.** No practical technology exists to detect someone carrying explosives onto a subway or a bus the way four men did in London 12 days ago, federal authorities said on Monday, July 18. The most effective method for finding explosives in a backpack or on a person boarding a subway or bus remains the use of dogs trained to sniff explosives, said officials from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). Bomb−sniffing dogs are used by a number of agencies, but there are only about 100 ATF−trained "explosives−detection canines" nationwide. Experts also said the bomb−sniffing dogs are limited in their abilities by a range of factors, including the strength of the explosive's odor and how far away the dogs are from a person carrying a bomb. Private companies, government agencies and scientists at U.S. laboratories and defense research centers are working to develop technologies that could possibly be used on mass−transit systems that carry 14 million people to work every day. After the London bombings, transit officials in Washington, DC stepped up security using dogs, cameras and police toting automatic weapons. But even its most sophisticated equipment −− the PROTECT system of chemical sensors installed at half of Metro's underground stations −− is not designed to prevent an attack but rather to minimize casualties and reduce the impact of a chemical release.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07 /18/AR2005071801291.html

9. *July 19, Associated Press* — **Aloha Airline reports $2.5 million profit.** Citing lower fuel costs and salary expenses, Aloha Airlines posted a $2.5 million operating profit in May, reversing a $3.8 million operating loss in April. Aloha, which filed for bankruptcy reorganization in December 2004, also lowered its year−to−date losses to $4.7 million from $7.2 million in April, according to a bankruptcy court filing made public Friday, July 15. "These numbers indicate that Aloha's reorganization plan is on course," said company spokesperson Stu Glauberman. The privately held Aloha said its overall expenses dropped to about $36 million in May from the previous month's $38.8 million. Its monthly fuel costs dropped to about $9 million from April's $9.4 million. Salary expenses for management and rank−and−file employees fell to $5.6 million from about $8.4 million in the previous month. Aloha, the state's second−largest airline with more than 3,600 employees and annual revenues of about $400 million, lowered its payroll cost with a 20% cut in executive salaries and wage concessions from its unionized employees.
Source: http://www.usatoday.com/travel/news/2005−07−18−aloha−earning_x.htm

10. *July 19, Associated Press* — **Note prompts jetliner return to Ft. Lauderdale.** An American Airlines flight to San Juan returned to Fort Lauderdale, FL, after about an hour when a threatening note was found on board. FBI spokesperson Judy Orihuela said flight 605 took off from Fort Lauderdale−Hollywood International Airport at 6:53 p.m. (EDT) on Monday, July 18. It turned back when someone reported discovering a piece of paper with a bomb threat written on it. Orihuela said the note was on a food services cart. The plane returned and was searched. Passengers were re−screened before resuming the flight.
Source: http://www.wofl.com/_ezpost/data/21899.shtml

11. *July 19, Associated Press* — **Authorities allege 40 pilots lied to fly, get medical certificates.** An 18−month investigation has resulted in the arrests of 40 Northern California pilots who may have been flying with debilitating illnesses that should have kept them grounded, the U.S. Attorney's office said. The pilots were receiving disability payments for serious medical conditions while maintaining active pilots' licenses, authorities allege. All the pilots, including commercial and transport pilots, claimed to be medically fit to fly an airplane while collecting disability payments from the Social Security Administration, Marlon Cobar, a prosecutor with the U.S. Attorney's office in Fresno, said Monday, July 18. Illnesses ranged from schizophrenia and bipolar disorder to drug and alcohol addiction and heart conditions −− all of which would disqualify them from holding a medical certificate, which is necessary to maintain a valid pilot's license. Federal Aviation Administration spokesperson Donn Walker said it was unclear how many of the pilots flew for a living, but that at least a dozen of them held commercial or airline transport licenses.
Source: http://www.usatoday.com/travel/news/2005−07−19−pilots−lied_x .htm

12. *July 18, San Bernardino County Sun (CA)* — **Border operation in works.** Hundreds of volunteers will monitor the California−Mexico border for illegal crossings starting in mid−September. Like the Minuteman Project in April at the Arizona border, Friends of the Border Patrol Border Watch is one of several civilian patrol groups that have recently organized to show dissatisfaction with the federal government's handling of illegal immigration. Almost 800 people, mainly from California, have signed up for the operation, scheduled to start September 16. Last weekend, another civilian border−watch group convened to monitor illegal crossings near El Campo, east of San Diego. The Minuteman Project also is expected to start patrolling the border of California, with all other Southern states, for one month in October. Many Border Watch participants will be camping in tents on site and the exact stretches of border to be patrolled have not been announced. Andy Ramirez founded Friends of the Border Patrol last summer following the Temecula Border Patrol station's arrests of hundreds of illegal residents in the streets of inland areas that included Ontario and Corona, CA.
Source: http://www.sbsun.com/Stories/0,1413,208~12588~2970886,00.htm l

13. *July 18, Reuters* — **EU approves air passenger data deal with Canada.** European Union (EU) foreign ministers approved on Monday, July 18, an EU−Canada deal that would allow authorities to collect passengers' personal data despite objections from the European Parliament. Under the accord, airlines flying from the European Union to Canada will transfer some passenger data to the Canadian authorities to help identify passengers who could be a security, and in particular a terrorist, threat, the European Commission said. But the agreement has angered EU lawmakers, who have taken legal action against a similar deal between the EU and United States, which they say violates privacy rights. The assembly says it would be best to

wait for the ruling from European Court of Justice before going ahead with any more deals to exchange sensitive passenger data with non−EU states. Brussels and Washington agreed in May 2004 to let U.S. authorities access airlines' booking records, scan up to 34 pieces of data for each passenger and keep them for 3−1/2 years. Fewer personal details are asked for under the EU−Canada agreement, which the Commission said respected European rules on data protection.
Source: http://www.vivelecanada.ca/article.php/20050718155757580

[Return to top]

Postal and Shipping Sector

14. *July 19, Journal Gazette (IN)* — **Fort Wayne receives detection system.** The Post Office in Fort Wayne, IN, is getting biohazard detection systems for its mail. Ed LaRocque, Allen County emergency management agency (EMA) director, told the Allen County EMA board Monday, July 18, that the post office will be installing anthrax testing machines in September. The detection system performs a rapid DNA test for anthrax and provides immediate notification if the substance is detected. Fort Wayne's downtown post office will be getting the machines, and they will be placed in buildings where mail is canceled. LaRocque said every piece of mail processed in Fort Wayne will go through the machines.
Source: http://www.fortwayne.com/mld/fortwayne/news/local/12168041.h tm

15. *July 18, Independent Newspapers (AZ)* — **Mail theft decreases in Mesa.** Cases of mail theft in Mesa, AZ, and the entire Valley, have decreased in the last two years, according to the U.S. Postal Inspection Service. In 2003, Mesa had 93 cases of mail theft reported. In 2004, reports in Mesa were down to 70 and as of July 5, only 43 reports had been filed for Mesa this year. "Mail theft in the Phoenix−metropolitan area is on the decline," said Patricia Armstrong, inspections service public information officer. Until about 2003, the Phoenix−metropolitan area led the nation in mail thefts. Methamphetamine use has been linked to nearly all mail theft cases reported in the Valley. "Here in Arizona there is a direct correlation to methamphetamine use and sale to mail theft," Armstrong said. "Nearly everyone ever arrested for the crime has been using or selling meth." The U.S. Postal Service has expanded its inspections service staff over the last few years and has invested $12 million in installing about 5,000 new and more secure cluster mail boxes across the Valley, including east Mesa. Armstrong credits those efforts for the decrease in mail thefts since 2003.
Source: http://www.newszap.com/articles/2005/07/18/az/east_valley/em 05.txt

[Return to top]

Agriculture Sector

16. *July 19, Iowa Ag Connection* — **Texas A&M leads world in cloning animals.** Through painstaking experimentation, Texas A&M is the world's first academic institution to clone six species in six years: cattle, a boer goat, pigs, a deer, a horse and −− most famously −− a cat named "cc." A&M scientists say the cloning research could result in the creation of disease resistant livestock, saving the agriculture industry millions of dollars and increasing food

production. Yet A&M's success has fueled the debate about the growing use of cloning, whether it is unnecessarily cruel to animals and whether the potential benefits are overblown. The cloning team harvests eggs from animal ovaries −− a delicate procedure that is performed with micromanipulators, or a high−tech microscope that holds an unfertilized egg in place while its nucleus is removed and a cultured cell is put inside. The cell and egg are then fused through electric stimulation to create an embryo that is implanted in the uterus of a surrogate mother. However, despite all the technological breakthroughs, cloning remains an inefficient process, according to Mark Westhusin, lead researcher with the A&M cloning team. Only one percent to five percent of cloning procedures succeed.
Source: http://www.iowaagconnection.com/story−national.cfm?Id=723&yr =2005

17. *July 18, National Academies* — **Reports call for high−level coordination of animal health and more research−oriented veterinarians.** The U.S. needs a new high−level mechanism to coordinate the currently fragmented framework for confronting new and emerging animal−borne diseases, such as mad cow disease, avian influenza, and West Nile virus, says a new report from the National Academies' National Research Council. Also, a second Research Council report released July 18 says stronger efforts are needed to recruit more veterinarians and other scientists into veterinary research. Both reports note that a growing shortage in the number of veterinary pathologists, lab animal scientists, and other veterinary researchers is making it more difficult to meet mounting challenges in animal health. The recently confirmed case of bovine spongiform encephalopathy (BSE) in June 2005 illustrated the potential economic impact of disease outbreaks, as some countries closed their markets to U.S. beef and beef products. Emerging diseases and the possibility of bioterrorism targeted at the food supply are among the evolving threats that challenge the U.S. animal health framework. Currently, dozens of federal and state agencies, university laboratories, and private companies monitor and maintain animal health in this country. Many of the government agencies perform similar functions, while gaps in responsibility also exist, particularly in federal oversight of nonlivestock animal diseases.
Source: http://www4.nationalacademies.org/news.nsf/isbn/0309097185?O penDocument

18. *July 18, North Dakota Ag Connection* — **North Dakota's anthrax case area enlarging.** Livestock owners in southeastern North Dakota have been urged to consider having their animals vaccinated for anthrax. "On July 6, anthrax was confirmed in two herds in Ransom County," said Dr. Beth Carlson, Deputy State Veterinarian. "Since then several additional cases of the disease have been confirmed in the area, which now includes southern Barnes County. Suspect cases have been reported in eastern Dickey and LaMoure counties as well." The anthrax−infected herds have been quarantined and are being vaccinated. Most cases have involved cattle; however, horses, bison, and farmed elk have also been affected. Carlson said anthrax has occurred in this area in the past, however, premises with no previous history of anthrax are being confirmed by the Veterinary Diagnostic Laboratory at North Dakota State University.
Source: http://www.northdakotaagconnection.com/story−state.cfm?Id=46 0&yr=2005

19. *July 18, Wisconsin Ag Connection* — **Wisconsin governor declares statewide drought emergency.** For the first time in nearly two years, Wisconsin Governor Jim Doyle has declared a statewide drought emergency. The executive order, which was signed by Doyle on Friday, July 15, will allow the Department of Natural Resources (DNR) to expedite farmers' requests

for temporary irrigation permits to divert stream or lake water to irrigate their parched crops, while assuring that fish and other aquatic life and water users aren't hurt by the requested diversions. "Wisconsin's drought conditions are stressing crops at a critical point in the growing season, and continued lack of rain could result in significant damage to our crops and severe economic losses for our farmers," Governor Doyle said. Under the executive order, the temporary irrigation permits would be in effect until August 14. In addition, the DNR is required to conduct a field inspection of the stream or lake proposed for diversion within 72 hours of receiving the request.
Source: http://www.wisconsinagconnection.com/story−state.cfm?Id=853& yr=2005

[Return to top]

Food Sector

20. *July 19, USAgNet* — **California proposes legislation to perform it's own bovine spongiform encephalopathy testing.** In the wake of the U.S. Department of Agriculture's (USDA) disclosure last month that the first U.S.−born bovine spongiform encephalopathy (BSE)−infected cow had been found on a ranch in Texas, Senator Mike Machado (D−CA) introduced new legislation in the California State Senate to permit ranchers to independently test their herd for BSE in order to guarantee the beef's safety to consumers. In addition to the Machado proposal, another California legislator, Assemblyman Paul Koretz (D−CA), has re−introduced a country−of−origin labeling proposal for meat sold in California. Furthermore this week, a recall disclosure bill introduced by Senator Jackie Speier (D−CA) is set for a vote in an Assembly committee. None of these proposals is supported by mainstream agriculture in California, which is the most agriculturally productive state in the U.S.
Source: http://www.usagnet.com/story−national.cfm?Id=721&yr=2005

[Return to top]

Water Sector

21. *July 19, Associated Press* — **Home Depot to buy National Waterworks.** Home Depot Inc., the world's largest home improvement retailer, said Tuesday, July 19, that it agreed to acquire water system supplier National Waterworks Holdings Inc. National Waterworks distributes products used to build, repair, and maintain water and wastewater transmission systems, and has a 14 percent share of the $11 billion market, according to Home Depot. The acquisition adds to Home Depot's earlier purchase in June of USABluebook, a leading national catalog distributor of maintenance, repair and operations supplies for the water and wastewater treatment industry. The company expects the transaction to close by the end of August.
Source: http://www.businessweek.com/ap/financialnews/D8BEEV800.htm?campaign_id=apn_home_down&chan=db

[Return to top]

Public Health Sector

22. *July 19, Agence France Presse* — **Vietnam to buy 415 million doses of bird flu vaccine.** Vietnam will buy 415 million doses of bird flu vaccine to inoculate poultry, state media said, in an attempt to limit the recurrence next winter of a virus has that killed 39 people in Vietnam. The Vietnam News Agency (VNA) said Tuesday, July 19, that the ministry of Agriculture and Rural Development would purchase the vaccine from China and the Netherlands. Vaccine would be "supplied to localities based on the number of their poultry stock and not sold on the market," VNA said. According to the ministry's plan, all breeding stock, poultry raised for meat and eggs, and fighting cocks must be vaccinated against the disease. The agriculture ministry also ordered that all chickens should be confined in cages and ducks in closed areas after being vaccinated. The vaccination program would start in August in southern Tien Giang province and northern Nam Dinh province, before being extended to the whole country later in the year.
Source: http://news.yahoo.com/s/afp/20050719/hl_afp/vietnamhealthflu_050719114533

23. *July 18, Guardian (United Kingdom)* — **U.S. to clamp down on foreign researchers.** The Pentagon has alarmed some U.S. scientists by proposing new restrictions on access to sensitive technology by foreign researchers. The large number of foreign researchers active in U.S. laboratories would have to wear badges and laboratories would have to contain segregated work areas under the proposed code. U.S. universities, which have been struggling to create a more welcoming climate for overseas postgraduate students and researchers in the wake of the 9/11 clampdown, believe the measures are excessive and could offend foreign scientists. In a memo urging its members to object to the Department of Defense proposals, the Association of American Universities (AAU) said the rules could easily spread beyond areas where there may be any security concern. The AAU noted that many universities were already experiencing "significant problems" with "troublesome clauses" in Pentagon research contracts. The association warned that the Pentagon would use the new rules to include "overly restrictive language" in many contracts.
Source: http://education.guardian.co.uk/higher/worldwide/story/0,995 9,1531112,00.html

24. *July 18, Reuters* — **Influenza drug may suppress Asian bird flu.** Roche's influenza drug Tamiflu suppresses the often deadly avian flu strain seen in Vietnam, U.S. researchers said on Monday, July 18. They said tests in mice showed the drug, licensed for use against influenza in general, could suppress the newest strain of H5N1 virus. The H5N1 strain has killed more than 50 people in Asia since 2003. "We need to know whether antiviral drugs can prevent and treat avian flu, because in the early stages of a global outbreak, most people would be unvaccinated," said Anthony Fauci, head of the National Institute of Allergy and Infectious Diseases, which funded the study. The team at St. Jude Children's Research Hospital in Memphis, TN, tested 80 mice with the drug, known generically as oseltamivir. None of the mice that got a placebo and then were infected with the Vietnam strain of H5N1 survived. Five of 10 mice given the highest daily dose of oseltamivir for five days survived. The researchers said eight of 10 mice given the drug for eight days lived. This will help experts decide how much drug to use and how long to treat people should the virus begin to spread among humans.
Report: http://www.journals.uchicago.edu/JID/journal/issues/v192n4/34183/brief/34183.abstract.html
Source: http://msnbc.msn.com/id/8617326/

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

25. *July 18, Quad City Times (IA)* — **Iowa town holds festival to raise money for emergency services.** With emergency medical technicians, registered nurses, first responders and paramedics, it would seem that the Wilton First Responders in Wilton, IA, were well−situated to serve the community in times of need. However, the organization says it needs equipment and certification to help Wilton residents to the fullest extent. This is why proceeds of the 2005 Wilton Community Festival will go directly to Wilton First Responders. A First Responder status allows one to provide the most basic medical care. Many Wilton First Responders are qualified far beyond first responder status, but can only practice at a first responder level because the group as a whole is certified as such. As a result, many of Wilton's First Responders are overqualified and by law cannot provide care which many of them are capable of doing. "We need to raise the department to a paramedic level so we can actually render better emergency aid at a scene at a higher level than we can now," said Beth Walker, a Wilton First Responder. However, raising the level of certification is expensive.
Source: http://www.qctimes.net/articles/2005/07/18/news/hometowns/doc42db36ce8a2fc459196034.txt

[Return to top]

Information Technology and Telecommunications Sector

26. *July 19, Federal Computer Week* — **NIST officials invite comment on draft standard.** Computer scientists at the National Institute of Standards and Technology (NIST) have released draft versions of two documents that they consider to be among the most important in a recent series of NIST documents on information security. One is a small publication describing minimum security requirements that will become mandatory after the Commerce Department secretary signs the document, as he is expected to do at the end of this year. That document is "Draft Federal Information Processing Standard (FIPS) Publication 200: Minimum Security Requirements for Federal Information and Information Systems." A second document, "Draft Special Publication 800−53A: Guide for Assessing the Security Controls in Federal Information Systems," is a 152−page guide to developing a cost−effective information security program based an agency’s assessment of its risks. Both documents are meant to help federal agencies secure their information systems and comply with the Federal Information Security Management Act (FISMA) of 2002, NIST officials said.
NIST will accept comments on "Draft Special Publication 800−53A" until August 31 at sec−cert@nist.gov: http://csrc.nist.gov/publications/drafts/sp800−53A−ipd.pdf
NIST will accept comments on "Draft FIPS Publication 200" until September 13 at draftfips200@nist.gov: http://csrc.nist.gov/publications/drafts/FIPS−200−ipd−07−13− 2005.pdf
Source: http://www.fcw.com/article89611−07−18−05−Web

27. *July 19, ComputerWeekly* — **Mobile phones of little use in crisis.** The London bombing highlighted important gaps in business continuity plans, according to security experts. Many firms discovered, to their cost, that their business continuity plans relied on being able to communicate with key staff via mobile phone networks, which were out of action or unreliable for most of the day the bombs exploded. Others found themselves in difficulty when key staff were unable to make it into work, said Andy Tomkinson, a director at the Business Continuity Institute. In the aftermath of the explosions police invoked a system called Access Overload Control, which shuts down large swathes of the mobile network, to free−up communications for the emergency services. Corporate e−mail systems also came under strain, which in some cases caused severe disruption to businesses. Some companies instructed staff to send text messages rather than make mobile phone calls−−a lesson learned from the central London power cut two years ago. Analyst firm Gartner said that the attacks showed that organizations need to have viable, tested business continuity plans, which are focused on people, not just business assets.
Source: http://www.computerweekly.com/Articles/2005/07/19/210901/Mobilephonesoflittleuseincrisis.htm

28. *July 19, IDG NEWS SERVICE* — **Attackers turning to fake online greeting cards.** According to Internet security vendor SurfControl PLC, attackers are increasingly using fake e−mail greeting cards as a way of getting malicious software installed on computers. In fact, the amount of malicious e−mail being disguised as e−mail greeting cards is up about 90% from last year and now makes up more than half of all malicious e−mail being sent, according to Paris Trudeau, a product marketing manager at SurfControl. The number of "phishing" attacks, in which users are tricked into entering personal information on fake Websites, is also on the rise. But increasingly, attackers are looking for ways to trick users into downloading software that can be used to take over a computer, turning it into a so−called zombie machine, she said. Often this can be done by sending an e−mail greeting that entices users to visit a maliciously encoded Web page, Trudeau said. Another trick is to mask an e−mail message so it appears to originate from the user's IT department.
Source: http://www.computerworld.com/securitytopics/security/holes/story/0,10801,103326,00.html

29. *July 18, US−CERT* — **Vulnerability Note VU#973635: SSH Communications Security SSH Tectia Server on Windows allows local access to host identification key.** SSH Tectia Server for Microsoft Windows creates the hostkey with permissions that allow any user to read the file. As a result, any user logged into the system can read the private SSH hostkey. Previous versions of SSH Tectia Server were known as SSH Secure Shell for Windows Servers. The hostkey is used to authenticate the server to the client. This defends against redirection attacks, such as DNS hijacking that cause the client to connect to a malicious server. In such cases, clients that know the public hostkey can verify that the server has the private hostkey, thereby verifying the server is correct. If an attacker copies the private hostkey of a server, they can configure a server with the same private key as the legitimate server. Such a server would appear valid to clients if another attack, such as DNS hijacking, was used to trick the client into connecting to the attacker's server.
Users should upgrade to SSH Tectia server 4.3.2 or later:
http://www.ssh.com/company/newsroom/article/653/
Source: http://www.kb.cert.org/vuls/id/973635

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT noted that a number of new exploits came out this weekend. If you are using applications vulnerable to these exploits, ensure you patch and update your software. A new Sybase vulnerability was reported which could give a remote attacker the capability to execute code with administrator privileges. Microsoft has been aware of and working on fixing a Remote Desktop Protocol (RDP) vulnerability since May, but has not released a fix yet. Some scanning of Port 3389, associated with RDP, was noted over the weekend. We recommend you take one or more of the actions recommended by Microsoft (see below) to mitigate this vulnerability.

Current Port Attacks

Top 10 Target Ports	1026 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 27015 (halflife), 135 (epmap), 139 (netbios−ssn), 1433 (ms−sql−s), 80 (www), 4672 (eMule), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

30. *July 19, Times (United Kingdom)* — **German court frees top bin Laden aide.** A suspected al Qaeda operative was released from jail in Germany Monday, July 18, after the country's highest court blocked his extradition to Spain on a new European Union (EU) arrest warrant. The Federal Constitutional Court ruled that Mamoun Darkazanli, a Syrian−German businessman, was entitled to protection under a law which says that German citizens cannot be extradited for trial abroad. Darkazanli was released from custody in Hamburg a few hours later. The ruling appears to deal a severe blow to pan−European efforts to co−ordinate the fight against terrorism. The whole architecture of the European arrest warrant −− a key component in counter−terrorism strategy −− was left looking distinctly shaky. Spain accuses Darkazanli of being Osama bin Laden's "permanent interlocutor and assistant" in Europe. Spanish authorities

believe that he had close contact with the terrorists who organised the attacks on the Madrid trains on March 11, 2004. Darkazanli is alleged to have been bin Laden's confidant since 1997 and to have conducted business deals for al Qaeda in Germany, Spain, and Kosovo. He appears in a wedding video with two of the three suicide pilots involved in the September 11 attacks, Marwan al−Shehhi and Ziad Jarrah, who lived and studied in Hamburg along with Mohammed Atta, the leading hijacker.
Source: http://www.timesonline.co.uk/article/0%2C%2C3−1699129%2C00.h tml

31. *July 19, Reuters* — **Pakistan detains 25 in London bomb probe raids.** Pakistani security forces detained 25 suspected Islamist militants in a series of raids linked to investigations into the July 7 bomb attacks in London, England, officials said on Tuesday, July 19. The latest detentions were made in an overnight crackdown in the most populous province, Punjab, and included members of outlawed Islamist groups. The death toll from the London underground train and bus bombings stood at 56 on Monday, July 18. Three of the four bombers were young British Muslims of Pakistani descent, and officials say all of them entered Pakistan through the southern city of Karachi last year. The fourth attacker was a Jamaican−born Briton. Out of 25 picked up overnight, four members of Sunni Muslim militant Lashkar−e−Jhangvi (Army of Jhangvi) group were formally arrested because they were wanted for crimes. Pakistan's President Pervez Musharraf ordered police to crack down on militant groups and hate literature in the days after Pakistani connections to the London bombs were first uncovered last week. On Monday, he accused banned militant organizations Jaish−e−Mohammad (Army of Mohammad) and Sipah−e−Sahaba (Soldiers of Mohammad's Companions) of forcing their ideology upon others, although he did not link them to the London bombings.
Source: http://reuters.myway.com/article/20050719/2005−07−19T121223Z _01_N19326016_RTRIDST_0_NEWS−SECURITY−BRITAIN−PAKISTAN−DC.ht ml

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer